ELSEVIER

Discrete Mathematics 238 (2001) 67–80

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

On t-designs from codes over Z_4

Tor Helleseth[a,*,1], Chunming Rong[b,1], Kyeongcheol Yang[c,2]

[a] *Department of Informatics, University of Bergen, Høyteknologisenteret, N-5020 Bergen, Norway*

[b] *Department of Electrical and Computer Engineering, Stavanger University College, P.O. Box 2557, N-4091 Stavanger, Norway*

[c] *Pohang University of Science and Technology, San 31 Hyoja-dong, Nam-gu, Pohang, Kyungbuk 790-784, South Korea*

Received 5 August 1999; revised 3 March 2000; accepted 1 June 2000

Abstract

There has been active research on t-designs constructed from codewords in codes over Z_4. We present an overview of the recent developments in constructing and proving such designs.

Keywords: Linear codes over Z_4; t-designs

1. Introduction

A t-design with parameters t-(v,k,λ) consists of subsets of size k (called blocks) from a set of v elements, such that for any t different elements there are precisely λ blocks that contain all t elements. A t-design is *simple* if it has no repeated blocks.

A linear code $\mathscr{C}$ over Z_4 (the ring of integers modulo 4) with block length n is an additive subgroup of Z_4^n. Let $T=\{T_1,T_2,\ldots,T_i\}$ be a set of any i arbitrary coordinates of $\mathscr{C}$. Then we will denote the punctured code of $\mathscr{C}$ at T by $\mathscr{C}^T$ and the shortened code of $\mathscr{C}$ at T by $\mathscr{C}^{0@T}$. The $\{0,2\}$-subcode of $\mathscr{C}$, which consists of codewords having only 0 or 2 as its elements is denoted by $\mathscr{C}_{[0,2]}$. Denote also $C^{(2)}=\{\frac{1}{2}\boldsymbol{c}\,|\,\boldsymbol{c}\in\mathscr{C},\boldsymbol{c}\equiv 0 \pmod 2\}$. The Gray map $\phi: Z_4\to Z_2^2$ is defined by $\phi(0)=00$, $\phi(1)=01$, $\phi(2)=11$, and $\phi(3)=10$. In general, the binary code defined by $C=\phi(\mathscr{C})$ is a non-linear binary code of length $2n$.

* Corresponding author.
E-mail address: tor.helleseth@ii.uib.no (T. Helleseth).

[1] This work was presented in part in the Third Shanghai Conference on Designs, Codes and Finite Geometries, China, May 14–18, 1999.

[2] This work was supported in part by the BK21 program of the Ministry of Education of Korea.

0012-365X/01/$ - see front matter
PII: S0012-365X(00)00417-9

Let R_m be a Galois ring of characteristic 4 with 4^m elements and let R_m^* be the set of units of R_m. R_m^* has a multiplicative cyclic subgroup $\mathscr{T} = \{1, \beta, \ldots, \beta^{2^m-2}\}$ of order $2^m - 1$, where $\beta \in R_m^*$ is an element of order $2^m - 1$. Let $\mathscr{T}_m = \mathscr{T} \cup \{0\}$. Any element $z \in R_m$ can be expressed uniquely as $z = A + 2B$ for $A, B \in \mathscr{T}_m$. Let μ denote the modulo-2 reduction map. Note that $\mu(\beta)$ is a primitive element in the finite field F_{2^m} with 2^m elements, thus $\mu(\mathscr{T}_m) = F_{2^m}$ (see [8] for details). The *trace* of z, $T(z)$, from R_m to Z_4 is defined by

$$T(z) = \sum_{j=0}^{m-1} \sigma^j(z).$$

There are several different weights used for codes over Z_4, namely the Hamming weight, the Lee weight and the Euclidean weight. The Hamming weight of a codeword is just the number of non-zero components. The Lee weights of the elements $0, 1, 2, 3$ in Z_4 are $0, 1, 2, 1$, respectively; and the Lee weight of a vector $\boldsymbol{a} \in Z_4^n$ is defined to be the sum of the Lee weights of its components. The Euclidean weights of the elements $0, 1, 2, 3$ in Z_4 are $0, 1, 4, 1$, respectively; and the Euclidean weight of a codeword is just the rational sum of the Euclidean weights of its components.

Let $\boldsymbol{c} = \{c_1, c_2, \ldots, c_n\}$ be a codeword of a linear code over Z_4. Define the multiplicity of i in $\boldsymbol{c}$ by $n_i(\boldsymbol{c}) = |\{c_k = i \mid 1 \leqslant k \leqslant n\}|$. Then the complete weight (enumerator) of $\boldsymbol{c}$ is defined as $W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})} Y^{n_2(\boldsymbol{c})} Z^{n_3(\boldsymbol{c})}$. Similarly, the symmetrized weight (enumerator) of $\boldsymbol{c}$ is defined as $W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})+n_3(\boldsymbol{c})} Y^{n_2(\boldsymbol{c})}$ and the Hamming weight (enumerator) as $W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})+n_2(\boldsymbol{c})+n_3(\boldsymbol{c})}$. Denote the codeword type of $\boldsymbol{c}$ by excluding the W factor, for example $X^{n_1(\boldsymbol{c})} Y^{n_2(\boldsymbol{c})} Z^{n_3(\boldsymbol{c})}$ for cwe-type. There are several useful weight enumerators for $\mathscr{C}$. The *complete weight enumerator* (or cwe) of $\mathscr{C}$ is defined as

$$\mathrm{cwe}_{\mathscr{C}}(W, X, Y, Z) = \sum_{\boldsymbol{c} \in \mathscr{C}} W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})} Y^{n_2(\boldsymbol{c})} Z^{n_3(\boldsymbol{c})}.$$

The *symmetrized weight enumerator* (or swe) of $\mathscr{C}$ is defined as

$$\mathrm{swe}_{\mathscr{C}}(W, X, Y) = \sum_{\boldsymbol{c} \in \mathscr{C}} W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})+n_3(\boldsymbol{c})} Y^{n_2(\boldsymbol{c})}.$$

The *Hamming weight enumerator* (or hwe) of $\mathscr{C}$ is defined as

$$\mathrm{hwe}_{\mathscr{C}}(W, X) = \sum_{\boldsymbol{c} \in \mathscr{C}} W^{n_0(\boldsymbol{c})} X^{n_1(\boldsymbol{c})+n_2(\boldsymbol{c})+n_3(\boldsymbol{c})}.$$

The *support* of a codeword $\boldsymbol{c}$ is the subset of $\{1, 2, \ldots, n\}$ given by $\{i \mid c_i \neq 0\}$. If we select codewords of the same support size k from a code, it may be possible to construct t-designs with $v = n$ for an integer t.

In this paper, we give an overview of the methods and the new designs constructed recently from codes over Z_4 described in Hammons et al. [8].

A recent interest in constructing t-designs from linear codes over Z_4 began when Harada [7] discovered through computer search, that the supports of codewords of Hamming weight 10 in certain extremal Type II codes of length 24 over Z_4, including

the Z_4-lifted Golay code G_{24}, form 5-$(24, 10, 36)$ designs. Subsequently, Harada [9] extended his previous result to the codewords of Hamming weight 12 in the Z_4-lifted Golay code G_{24} to find 5-$(24, 12, 1584)$ and 5-$(24, 12, 1632)$ designs through computer search. Bonnecaze et al. [4] proved that the supports of the codewords of constant symmetrized weight type in the lifted Golay code over Z_4 form 5-designs possibly with repeated blocks. They also introduced the notion of a colored t-design and constructed colored 5-designs from codewords of the same symmetrized weight in the various Type II codes over Z_4.

In Helleseth et al. [12,14] 3-designs are constructed and proved by using the support of small weight codewords in the Preparata codes over Z_4. In Helleseth and Yang [23], 3-designs are given by the support of the codewords of each type in the Kerdock codes over Z_4. In Helleseth et al. [15], some 3-designs are constructed and verified by computer search using the support of small weight codewords in the Goethals codes over Z_4. In Kreher [16], all known simple t-designs with $t \geqslant 3$ are listed. The parameters of the simple designs given in papers mentioned above are not listed in [16] and therefore appear to be new. Also the construction of the 3-designs is new. These designs are then later verified by Shin et al. [20] using a new Kloosterman sum identity.

More recently, Duursma et al. [6] concluded that, in both Preparata codes and Kerdock codes over Z_4, codewords of an arbitrary but fixed complete weight yield a 3-design (not necessarily a simple design).

The Assmus–Mattson theorem [1] gives sufficient conditions for the support of the codewords of constant weight in a linear code over a finite field to form a t-design. Efforts has also been made to find an analogue of the theorem for codes over Z_4. Shin et al. [19] give an Assmus–Mattson approach to designs from Z_4-linear codes on Hamming weight enumerator. The theorem can find 3-designs in the Kerdock and Preparata codes over Z_4, but cannot find 5-designs in the lifted Golay code G_{24}. They also obtained [20] more designs from the Goethals codes over Z_4. At the same time, Tanabe [21] gives a candidate of an Assmus–Mattson theorem for Z_4-codes using the symmetrized weight enumerator applying Bachoc's method in [2] which gives a new proof of the Assmus–Mattson theorem for linear binary codes. The theorem can find some 5-designs in G_{24}, but there is a difficulty to check when the code contains 5-designs. Using the methods of Shin et al. [19], Tanabe improves the result by giving, in [22], a criterion to find designs in Z_4-codes using the symmetrized weight enumerator.

2. 5-designs from Type II codes of length 24 over Z_4

The product of two elements, $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, of Z_4^n is defined by $x \cdot y = x_1 y_1 + \cdots + x_n y_n \bmod 4$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in Z_4^n \mid x \cdot y = 0,\ \forall y \in C\}$. C is *self-dual* if $C = C^\perp$.

Type II codes over Z_4 are self-dual codes containing the all-ones vector with the property that all Euclidean weights are divisible by 8. It is known that a Type II code

of length n exists if and only if $n \equiv 0 \bmod 8$. An upper bound $8(\lfloor n/24 + 1 \rfloor)$ on the minimum Euclidean weight of a Type II code of length n is given in Bonnecaze et al. [5]. A Type II code meeting this bound with equality is called *extremal* (cf. [5]). Extremal codes have the largest minimum Euclidean weight among all Type II codes of that length.

Defined in [3], the lifted Golay code G_{24} is constructed from the cyclic code of length 23 with generating polynomial $x^{11} + 2x^{10} + 3x^9 + 3x^7 + 3x^6 + 3x^5 + 2x^4 + x + 3$ by appending 3 to the last coordinate of the generator vectors. G_{24} is a self-dual code over Z_4.

By exhaustive computer search, Harada [7] discovered that the supports of codewords of Hamming weight 10 in certain extremal Type II codes of length 24 over Z_4, including the Z_4-lifted Golay code G_{24}, form 5-$(24, 10, 36)$ designs. Subsequently, Harada [9] extended his previous result to the codewords of Hamming weight 12 in the Z_4-lifted Golay code G_{24} to find 5-$(24, 12, 1584)$ and 5-$(24, 12, 1632)$ designs through computer search. Designs with these parameters were not known to exist before. There is also an interesting property associated with the 5-$(24, 10, 36)$ parameters. If there is an extremal Type IV code (also known as Hermitian self-dual code) over F_4 of length 24, then the minimum weight codewords of the code form a 5-$(24, 10, 36)$ design. However, the nonexistence of such a code is known [18].

Bonnecaze et al. [4] proved that the supports of the codewords of constant symmetrized weight type in the lifted Golay code over Z_4 form 5-designs possibly with repeated blocks. They also introduced the notion of a colored t-design and constructed colored 5-designs from codewords of the same symmetrized weight in the various Type II codes over Z_4.

3. Designs from Kerdock and Preparata codes over Z_4

The Kerdock code $\mathscr{K}_m$ of length 2^m over Z_4 is defined by

$$\mathscr{K}_m = \{c(a, b) \mid a \in R_m, b \in Z_4\},$$

where $c(a, b)$ is a vector in $Z_4^{2^m}$ indexed by the elements of $\mathscr{T}_m$ such that $c(a, b)_x = T(ax) + b$ for all $x \in \mathscr{T}_m$. Clearly, $\mathscr{K}_m$ has 4^{m+1} codewords. In [8], Hammons et al. showed that if m is odd, then $\mathscr{K}_m$ has minimum Lee weight $2^m - 2^{m-1/2}$ and its Gray map $\phi(\mathscr{K}_m)$ gives a $(2^{m+1}, 2^{2m+2}, 2^m - 2^{m-1/2})$ binary non-linear Kerdock code. The Lee weight distribution of $\mathscr{K}_m$ is well-known in [8].

Lemma 1. *Let m be an odd integer $\geqslant 3$ and let $\mathscr{K}_m$ be the Kerdock code of length $n = 2^m$ over Z_4. Then every codeword has one of the following types*:

(a) i^n, *one time for each* $i = 0, 1, 2, 3$;
(b) $2^{n/2}0^{n/2}$, $2(2^m - 1)$ *times*;
(c) $1^{n/2}3^{n/2}$, $2(2^m - 1)$ *times*;

(d) $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}, 2^m(2^m-1)$ *times, where* $n_1 = 2^{m-2} \pm 2^{(m-3)/2}$, $n_2 = 2^{m-2} - 2^{(m-3)/2}$, *and* $n_3 = 2^{m-2} \mp 2^{(m-3)/2}$;

(e) $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$, $2^m(2^m-1)$ *times, where* $n_1 = 2^{m-2} \pm 2^{(m-3)/2}$, $n_2 = 2^{m-2} + 2^{(m-3)/2}$, *and* $n_3 = 2^{m-2} \mp 2^{(m-3)/2}$.

Changing the sign of a codeword leads to a codeword with the same support. Hence, to construct simple designs (designs without repeated blocks), we only consider the codewords with $n_1 \geqslant n_3$ when $n_1 \neq 0$.

The next theorem shows that the support of the codewords of each type in the Kerdock code $\mathscr{K}_m$ over Z_4 form 3-designs for any odd integer $m \geqslant 3$. Clearly, the codewords of the types given in Lemma 1(a)–(c) give trivial 3-designs. It will be shown that two new infinite families are constructed from the codewords of the types given in Lemma 1(d) and (e), respectively.

It is well-known that the non-linear binary Kerdock code contains 3-designs [17, p. 456]. However, these 3-designs have different parameters than the 3-designs obtained from the Kerdock code $\mathscr{K}_m$ over Z_4 in the following two theorems.

Theorem 1. *The support of the codewords of the type* $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ *in the Kerdock code* $\mathscr{K}_m$ *of length* $n = 2^m$ *over* Z_4 *form a* 3-$(2^m, k, \lambda)$ *design for any odd integer* $m \geqslant 3$, *where*

$$k = 2^{m-1} + 2^{m-2} - 2^{(m-3)/2}, \quad \lambda = \frac{k(k-1)(k-2)}{2^m - 2}$$

and

$$n_1 = 2^{m-2} + 2^{(m-3)/2}, \quad n_2 = n_3 = 2^{m-2} - 2^{(m-3)/2}.$$

Theorem 2. *The support of the codewords of the type* $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ *in the Kerdock code* $\mathscr{K}_m$ *of length* $n = 2^m$ *over* Z_4 *form a* 3-$(2^m, k, \lambda)$ *design for any odd integer* $m \geqslant 3$, *where*

$$k = 2^{m-1} + 2^{m-2} + 2^{(m-3)/2}, \quad \lambda = \frac{k(k-1)(k-2)}{2^m - 2}$$

and

$$n_1 = n_2 = 2^{m-2} + 2^{(m-3)/2}, \quad n_3 = 2^{m-2} - 2^{(m-3)/2}.$$

The Preparata code $\mathscr{P}_m$ of length 2^m over Z_4 is the code over Z_4, whose parity-check matrix is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \end{bmatrix}. \tag{1}$$

In Hammons et al. [8], it is shown that if m is odd, then $\mathscr{P}_m$ has minimum Lee weight 6 and its Gray map $P_m = \phi(\mathscr{P}_m)$ gives a $(2^{m+1}, 2^{2^{m+1}-2m-2}, 6)$ binary non-linear

code. The binary code P_m has the same Hamming weight distribution as the original Preparata code [17]. The Kerdock code is the dual of the Preparata code.

A vector is said to be of the type $1^{n_1}2^{n_2}3^{n_3}0^{n_0}$ if i occurs n_i times, $i=0,1,2,3$, as a component. The codewords of minimum Lee weight in the Preparata code $\mathscr{P}_m$ for any odd integer m are of the type $1^3 2^1 3^1 0^{n-5}$ or $1^1 2^1 3^3 0^{n-5}$. Changing the sign of a codeword leads to a codeword with the same support. Hence, to construct simple designs (designs without repeated blocks), we only consider the former type. Note that the codewords in $\mathscr{P}_m$ of minimal Lee weight have Hamming weight 5.

Theorem 3 (Helleseth et al. [12]). *The support of the codewords of the type* $1^3 2^1 3^1 0^{n-5}$ (*or* $1^1 2^1 3^3 0^{n-5}$) *in the Preparata code* $\mathscr{P}_m$ *over* Z_4 *form a* 3-$(2^m, 5, 10)$ *design for any odd integer* $m \geqslant 3$.

There is another approach [14] to prove Theorem 3 without determining the λ-parameter, i.e. the minimum Lee weight codewords form a simple 3-$(2^m, 5, \lambda)$ design for an integer λ.

Codewords of the type $1^5 2^0 3^1 0^{n-6}$ or $1^4 2^2 3^0 0^{n-6}$ or $1^3 2^0 3^3 0^{n-6}$ or $1^2 2^2 3^2 0^{n-6}$ in the Preparata code $\mathscr{P}_m$, for m odd, are of support size 6. In a similar approach as given in the proof of Theorem 3, we constructed [14] the following simple 3-designs from these codewords of support size 6:

Theorem 4 (Helleseth et al. [14]). *In the Preparata code* $\mathscr{P}_m$ *over* Z_4 *for any odd integer* $m \geqslant 5$, *there are the following designs*:

(i) *The support of the codewords of type* $1^5 2^0 3^1 0^{n-6}$ *form a* 3-$(2^m, 6, 2^m - 8)$ *design.*
(ii) *The support of the codewords of type* $1^4 2^2 3^0 0^{n-6}$ *form a* 3-$(2^m, 6, 5 \cdot (2^{m-1} - 4))$ *design.*
(iii) *The support of the codewords of type* $1^3 2^0 3^3 0^{n-6}$ *form a* 3-$(2^m, 6, 20 \cdot (2^{m-1} - 4)/3)$ *design.*
(iv) *The support of the codewords of type* $1^2 2^2 3^2 0^{n-6}$ *form a* 3-$(2^m, 6, 18 \cdot (2^{m-1} - 4))$ *design*.

More recently, Duursma et al. [6] concluded that, in both Preparata codes and Kerdock codes over Z_4, codewords of an arbitrary but fixed complete weight yield a 3-design (not necessary simple design). That is codewords with given numbers of 0's, 1's, 2's and 3's. Let n_0, n_1, n_2, n_3 denote these numbers and $w_C = (n_0, n_1, n_2, n_3)$ the complete weight. The symmetrized weight of a codeword is defined by $w_S = (n_0, n_1 + n_3, n_2)$, the Hamming weight by $w_H = n_1 + n_2 + n_3$ and the Lee weight by $w_L = n_1 + 2n_2 + n_3$.

Theorem 5. *For the quaternary Kerdock or Preparata code of length* $N = 2^m$, m *odd, let* Ω *be the set of all codewords of a given complete weight. For any three distinct coordinates* $\sigma = (i, j, k)$ *and values* $e = (e_i, e_j, e_k)$ *at these coordinates, the number of*

words in Ω that agree on σ with either e or a permutation of e depends only on the values e and not on the coordinates σ.

Thus, the words of a given complete weight define blocks of a 4-colored 3-design. The theorem implies that the number of words in Ω that is non-zero on three given coordinates is independent of the chosen coordinates. Denoting this number by λ, the number of incidences of three coordinates with supports of codewords in Ω is counted in two different ways as $\binom{N}{3}\lambda = |\Omega|\binom{w}{3}$, which proves the following Theorem 6.

Theorem 6. *For the quaternary Kerdock or Preparata code of length $N = 2^m$, m odd, let Ω be the set of all codewords of a given complete weight and let w be the common Hamming weight of words in Ω. The number of words in Ω that is nonzero on three given coordinates is independent of the chosen coordinates and is given by*

$$|\Omega| \binom{w}{3} \Big/ \binom{N}{3}.$$

In other words, the words of complete weight define the blocks of a (2-colored) 3-design.

A different result is obtained by considering classes of codewords that have the same symmetrized weight. That is codewords with given numbers of 0's and 2's.

Theorem 7. *For the quaternary Kerdock or Preparata code of length $N = 2^m$, m odd, let Ω be the set of all codewords of a given symmetrized weight. For any three distinct coordinates $\sigma = (i, j, k)$ and values $e = (e_i, e_j, e_k)$ at these coordinates, the number of words in Ω that agree on σ with e depends only on the values e and not on the coordinates σ.*

Thus, the words of given symmetrized weight define blocks of a strong 3-colored 3-design. Both Theorems 5 and 7 are obtained [6] from properties of the cosets of the Preparata code. For the binary images under the Gray mapping, the latter theorem implies the classical result [25] that the words of a given Hamming weight in the binary Kerdock or Preparata code define a 3-design.

For Kerdock codes, the theorem on symmetrized weights can be shown [6] to be equivalent to the following theorem on complete weights. However, the result is not valid for Preparata codes.

Theorem 8. *For the quaternary Kerdock code of length $N = 2^m$, m odd, let Ω be the set of all codewords of a given complete weight. For any three distinct coordinates $\sigma = (i, j, k)$ and values $e = (e_i, e_j, e_k)$ at these coordinates, the number of words in Ω that agree on σ with either e or $-e$ depends only on the values e and not on the coordinates σ.*

4. Designs from Goethals codes over Z_4

The Goethals code $\mathscr{G}_m$ of length 2^m over Z_4 is the code over Z_4, whose parity-check matrix is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \cdots & 2\beta^{3(2^m-2)} \end{bmatrix}.$$

In Hammons et al. [8], it is shown that if m is odd, then $\mathscr{C}$ has minimum Lee distance 8 and its Gray map $G_m = \phi(\mathscr{G}_m)$ gives a $(2^{m+1}, 2^{2^{m+1}-3m-2}, 8)$ binary non-linear code, which has the same parameters as the original Goethals code [17]. The Goethals code has four times as many codewords as the comparable extended triple error-correcting primitive BCH code.

Let $(c_X)_{X \in \mathscr{T}_m}$ be a codeword of the Goethals code $\mathscr{G}_m$. Then it must satisfy

$$\sum_{X \in \mathscr{T}_m} c_X = 0, \qquad \sum_{X \in \mathscr{T}_m} c_X X = 0 \quad \text{and} \quad 2\sum_{X \in \mathscr{T}_m} c_X X^3 = 0. \tag{2}$$

These relations give the following invariant property of $\mathscr{G}_m$.

Lemma 2 (Hammons et al. [8]). *The Goethals code $\mathscr{G}_m$ is invariant under the doubly transitive group of 'affine' permutations of the form $X \to (AX + B)^{2^m}$, where $A, B \in \mathscr{T}_m$ and $A \neq 0$.*

Theorem 9. *The support of the codewords of the type $1^4 2^1 3^2 0^{n-7}$ in the Goethals code $\mathscr{G}_5$ over Z_4 form a 3-$(2^5, 7, 105)$ design. The support of the codewords of the type $1^6 2^1 3^0 0^{n-7}$ form a 3-$(2^5, 7, 7)$ design.*

Sketch of Proof. We only consider the codewords in $\mathscr{G}_5$ of type $1^4 2^1 3^2 0^{n-7}$ with support $\{X_1, \ldots, X_7\} \subset \mathscr{T}_m$. The proof of the other case is similar. We will show that for any three coordinates X_1, X_2 and X_3 in $\mathscr{T}_m$, there are exactly the same number, say λ, of codewords of this type with non-zero support at these coordinates. Since the Goethals code is invariant under the doubly transitive group of 'affine' permutations by Lemma 2, we can assume without loss of generality that the first two coordinates are $X_1 = 0$ and $X_2 = 1$. Furthermore, the third coordinate is choosen arbitrary to be $X_3 = A \in \mathscr{T}_m \setminus \{0, 1\}$. Let $x_j = \mu(X_j)$ and $a = \mu(A)$. Hence, $x_1 = 0$, $x_2 = 1$ and $x_3 = a$. Let $x_4 = y$. Note that $X_1, X_2, \ldots, X_7$ are distinct elements of $\mathscr{T}_m$ and $0, 1, a, y, x_5, x_6, x_7 \in F_{2^m}$ are therefore distinct.

Let U_{X_j} denote the non-zero values of such a codeword at the seven corresponding locations X_j for $j = 1, 2, \ldots, 7$. We will discuss the conditions for a codeword to have this support. For a such codeword, there are 19 possible ways for the values U_0, U_1 and U_A as listed in Table 1.

There are four classes in the table which are distinguished by Class I (Cases 1.1–1.7 with $U_{X_7} = 2$), Class II (Cases 2.1–2.3 with $U_{X_4} = 1$, $U_{X_5} = U_{X_6} = 3$ and $U_{X_7} = 1$), Class III (Cases 3.1–3.3 with $U_{X_4} = U_{X_5} = U_{X_6} = U_{X_7} = 1$), Class IV (Cases 4.1–4.6

Table 1
All possible U_0, U_1, U_A for codewords of the Type $1^4 2^1 3^2 0^{n-7}$

Case	U_0	U_1	U_A	U_{X_4}	U_{X_5}	U_{X_6}	U_{X_7}
1.1	1	1	1	1	3	3	2
1.2	1	1	3	3	1	1	2
1.3	1	3	1	3	1	1	2
1.4	3	1	1	3	1	1	2
1.5	3	3	1	1	1	1	2
1.6	3	1	3	1	1	1	2
1.7	1	3	3	1	1	1	2
2.1	1	1	2	1	3	3	1
2.2	1	2	1	1	3	3	1
2.3	2	1	1	1	3	3	1
3.1	3	3	2	1	1	1	1
3.2	3	2	3	1	1	1	1
3.3	2	3	3	1	1	1	1
4.1	1	3	2	3	1	1	1
4.2	3	1	2	3	1	1	1
4.3	3	2	1	3	1	1	1
4.4	1	2	3	3	1	1	1
4.5	2	1	3	3	1	1	1
4.6	2	3	1	3	1	1	1

with $U_{X_4} = 3$ and $U_{X_5} = U_{X_6} = U_{X_7} = 1$). If there is a 3-design, the cases in a same class will together give a constant number of codewords independent of the choice of A.

To determine the number of solutions of this system in each of the cases, we first transform, using the technique described in [10], the parity-check equations into a system of binary equations over F_{2^m}.

In Class I, it can be shown that each of the Cases 1.1–1.4 gives exactly $2^{m-1} - 4$ codewords and each of the Cases 1.5–1.7 gives exactly $(2^{m-1} - 4)/3$ codewords. In total, Class I gives $5 \cdot (2^{m-1} - 4)$ codewords. By computer search on $m = 5$, we verify that there are exactly 60 codewords for cases in Class I.

Each of cases in Classes II, III and IV may not give a constant number of codewords for each choice of A. However, by computer search on $m = 5$, we verify [13] that there are exactly 18 codewords for cases in Class II, 3 codewords for cases in Class III, 24 codewords for cases in Class IV, which are all independent of the choice of A.

Hence, for $m = 5$, we have verified by computer search that the support of the codewords of the type $1^4 2^1 3^2 0^{n-7}$ in the Goethals code $\mathscr{G}_m$ over Z_4 form a 3-$(2^5, 7, 105)$ design. Note that the block size $b = 105\binom{32}{3}/\binom{7}{3} = 14\,880$.

Remark. For $m = 7$, we have verified by computer search that neither the codewords of type $1^4 2^1 3^2 0^{n-7}$ nor the codewords of type $1^6 2^1 3^0 0^{n-7}$ in $\mathscr{G}_7$ form a 3-design. However, combining the codewords of both of these types leads to the following theorem.

Theorem 10. *The support of the codewords in $\mathscr{G}_7$ obtained by combining both of the types $1^4 2^1 3^2 0^{n-7}$ and $1^6 2^1 3^0 0^{n-7}$ form a 3-$(2^7, 7, 560)$ design.*

More recently, Shin et al. [20] obtained designs (both new and those constructed by us) from the Goethals codes over Z_4 by using Kloosterman sums. They derive a new infinite family of simple 3-designs from codewords of Hamming weight 7 of the same swe-type as given in the following theorem.

Theorem 11 (Shin et al. [20]). *The union of the supports of codewords of the cwe-types X^4YZ^2 and X^6Y in the Goethals code over Z_4 of length 2^m forms a simple 3-$(2^m, 7, \frac{14}{3}(2^m - 8))$ design for odd $m \geqslant 5$.*

The theorem yields (i) a 3-$(2^5, 7, 112)$ design which corresponds to the union of the 3-$(2^5, 7, 105)$ and the 3-$(2^5, 7, 7)$ designs in [14] and (ii) a 3-$(2^7, 7, 560)$ design which is identical to that in Theorem 10.

5. Assmus–Mattson type theorems over Z_4

The Assmus–Mattson theorem [1] gives sufficient conditions for the support of the codewords of constant weight in a linear code over a finite field to form a t-design.

Theorem 12 (Assmus–Mattson Theorem [1] or see MacWilliams and Sloane [17]). *Let C be a linear binary code of length n and minimum distance d and e be the minimum distance of $C^\perp$. Assume an integer $t < d$ satisfies the condition*

$$\#\{i \mid 0 \neq i \text{ is a Hamming weight of } C^\perp \text{ and } i \leqslant n - t\} \leqslant d - t.$$

Then, the support of the codewords of C (respectively $C^\perp$) of any Hamming weight w forms a t-design for $d \leqslant w \leqslant n$ (respectively $e \leqslant w \leqslant n - t$).

Efforts has also been made to find an analogue of the theorem for codes over Z_4. Shin et al. [19] presented an Assmus–Mattson type approach at identifying t-designs in linear codes over Z_4:

(1) Select a weight enumerator of $\mathscr{C}$ and $\mathscr{C}^\perp$ from amongst the complete, symmetrized, and Hamming-weight enumerators.
(2) The dual of the punctured code $\mathscr{C}^T$ at T is the shortened dual code $(\mathscr{C}^\perp)^{0@T}$ at T. If $\mathscr{C}^\perp$ has few weights (or weight types) and $\mathscr{C}$ has large minimum distance, the MacWilliams identities can often be used to identify the weight enumerator of the punctured code $\mathscr{C}^T$.
(3) If the weight enumerator of $\mathscr{C}^T$ is invariant of the choice of coordinates T for puncturing, then the codewords of constant Hamming weight in $\mathscr{C}$ form a t-design possibly with repeated blocks where $t = |T|$.

Applying this approach, Shin et al. [19] showed that the codewords of constant Hamming weight in both the Goethals code over Z_4 as well as the Delsarte-Goethals code over Z_4 yield 3-designs, possibly with repeated blocks. From a special case of the Assmus–Mattson type approach, corresponding to choosing the Hamming weight enumerator, they also give an Assmus–Mattson type theorem for linear codes over Z_4.

Theorem 13 (Shin et al. [19]). *Let $\mathscr{C}$ be a linear code over Z_4 of length q such that all codewords of constant Hamming weight in the $\{0,2\}$-subcodes $\mathscr{C}_{[0,2]}$ and $(\mathscr{C}^{\perp})_{[0,2]}$ of $\mathscr{C}$ and $\mathscr{C}^{\perp}$ yield t-designs. Let s be the number of non-zero weights in $(\mathscr{C}^{\perp}-(\mathscr{C}^{\perp})_{[0,2]})^{0@T}$ where $T\subset\mathscr{T}$ is of size t. Let d be the minimum Hamming weight in $(\mathscr{C}-\mathscr{C}_{[0,2]})$. Then the codewords of constant Hamming weight in $\mathscr{C}$ and the codewords of constant Hamming weight $\leqslant q-t$ in $\mathscr{C}^{\perp}$ yield t-designs possibly with repeated blocks as well provided $d-t\geqslant s$.*

The theorem can find 3-designs in the Kerdock and Preparata codes over Z_4, but cannot find 5-designs in the lifted Golay code G_{24}. They also obtained [20] more designs from the Goethals codes over Z_4.

At the same time, Tanabe [21] gives a candidate of an Assmus–Mattson theorem for Z_4-codes on the symmetrized weight enumerator by using Bachoc's method in [2] which gives a new proof of the Assmus–Mattson theorem for linear binary codes. The theorem can find some 5-designs in the lifted Golay code G_{24}, but there is a difficulty to check when the code contains 5-designs.

Using the methods of Shin et al. [19], Tanabe improves the result by giving, in [22], a criterion to find designs in Z_4-codes using the symmetrized weight enumerator.

Denote by $\boldsymbol{R}X$, $\boldsymbol{R}X_i$, and $\boldsymbol{R}V$ the free real vector spaces spanned by the elements of X, X_i, and V, respectively. For a Z_4-code $\mathscr{C}$ we denote by $\Gamma(\mathscr{C})$ the set of all Lee compositions (n_0,n_1,n_2) of $\mathscr{C}$ satisfying one of the following conditions:

(1) $n_1=0$.
(2) $n_1>0$ and there is no pair of Lee compositions of $\mathscr{C}$ $((a_0,a_1,a_2),(b_0,b_1,b_2))$ such that:
  (i) $a_1=b_1=0$, $a_2>0$, $b_2>0$, and $a_2+b_2=n_1$, or
  (ii) $a_1=b_1=2(n_1-a_2-b_2)$ and $n_2\geqslant n_1-a_2-b_2>0$.
(3) $n_1>0$ and there is no pair of Lee compositions of $\mathscr{C}$ of type (i) and there are pairs of Lee compositions of $\mathscr{C}$ of type (ii) in 2. For any Lee composition of $\mathscr{C}$ of type (ii) in 2, $(n-n_2-a_2-b_2,n_1,n_2-n_1+a_2+b_2)$ is not a Lee composition of $\mathscr{C}$.

For non-negative integers i,j,a,b, define

$$P_j^{(n-2k)}(i-k)=\sum_{m=0}^{j}\binom{i-k}{m}\binom{n-k-i}{j-m}3^{j-m}(-1)^m,$$

and the Krawtchouk polynomials,

$$Q^k(i,j;\ a,b) = \sum_{\substack{r,s,t\geqslant 0 \\ r\leqslant i,\ s+t\leqslant j}} \binom{n-k-i-j}{n-k-i-j-a-b+r+s+t,\ a-s,\ b-r-t} \binom{i}{r}\binom{j}{j-s-t,\ s,\ t,} (-1)^{r+s},$$

where

$$\binom{i}{i-j_1-j_2, j_1, j_2} := \frac{i!}{(i-j_1-j_2)!j_1!j_2!}.$$

Theorem 14 (Tanabe [22]). *Let $\mathscr{C}$ be a Z_4-code and e be the minimum Hamming distance of $\mathscr{C}^{\perp}$. Define*

$$\Lambda(k) = \{(n_1(\boldsymbol{c}), n_2(\boldsymbol{c})) \mid \boldsymbol{c}\in\mathscr{C},\ k\leqslant wt_{Hamming}(\boldsymbol{c})\leqslant n-k \text{ and } n_1(\boldsymbol{c})>0\},$$

$$\Lambda_1(k) = \left\{(a,b)\in\{1,\dots,n\}^2 \;\middle|\; \begin{array}{l} 0\leqslant a+b\leqslant n-k \text{ and} \\ a>n_1(\boldsymbol{c}) \text{ or } b>n_2(\boldsymbol{c}) \text{ for any } \boldsymbol{c}\in\mathscr{C}^{\perp} \end{array}\right\},$$

$$\Lambda_2(k) = \{c\in\{0,\dots,n-2k\} \mid c+k\in\{wt_{Hamming}(\boldsymbol{c}) \mid \boldsymbol{c}\in\mathscr{C}^{\perp} \text{ and } \boldsymbol{c}\not\equiv 0 \pmod 2\}\}.$$

Define matrices $M_1(k)\in \mathrm{Mat}_{\Lambda(k)\times\Lambda_1(k)}(\boldsymbol{R})$ whose $((n_1,n_2),\ (a,b))$th entry is $Q^k(n_1,n_2; a,b)$, $M_2(k)\in\mathrm{Mat}_{\Lambda(k)\times\Lambda_2(k)}(\boldsymbol{R})$ whose $((n_1,n_2),\ c)$th entry is $P_c^{(n-2k)}(n_1+n_2-k)$, and $M(k)=[M_1(k)\ M_2(k)]$.

Let t be a positive integer. Assume t satisfies the condition in Theorem 12 for two linear binary codes $C^{(2)}$ (or its dual) and $(C^{\perp})^{(2)}$ (or its dual) and that the rank of $M(k)$ is equal to its row length $(=\#\Lambda(k))$ for all k $(1\leqslant k\leqslant t)$. Then, the support of the codewords of $\mathscr{C}$ of any Lee composition $(n_0,n_1,n_2)\in\Gamma(\mathscr{C})$ with $t\leqslant n_1+n_2\leqslant n-t$ forms a t-design and the support of codewords of $\mathscr{C}^{\perp}$ of any Hamming weight l with $l-\lceil l/4\rceil < e$ forms a t-design.

There is a difficulty to know the ranks of $M(k)$ in the theorem in general. A simple sufficient condition to guarantee the matrices have full ranks is given in Corollary 1. A condition on Lee compositions is needed in the corollary.

Let h be a positive integer, γ be an integer with $0\leqslant\gamma\leqslant h$, $F_i(X,Y)\in\boldsymbol{R}[X,Y]$ $(1\leqslant i\leqslant\gamma)$ be homogeneous polynomials of degree h, and $\mathscr{A}$ be a finite subset of $\boldsymbol{R}^2$.

$\mathscr{A}$ is said to 'satisfy' the condition $(*)$ for $(h, \{F_i\}_{i=1}^{\gamma})$ if the following condition $(*)$ holds:

$$(*)\quad \begin{cases} \text{There is a set } J=\{j_1,\dots,j_\gamma\}\subset \boldsymbol{Z} \text{ with } 0\leqslant j_i\leqslant h, \text{ a set} \\ \mathscr{B}=\{(a_i,b_j)\in \boldsymbol{R}^2 \mid (i,j)\in \Delta(h,J)\} \text{ with } aq_i\neq a_j\ (i\neq j) \\ \text{and } b_i\neq b_j\ (i\neq j), \text{ and a } \sigma\in GL(2,\boldsymbol{R}) \text{ such that} \\ \bullet\ \sigma\mathscr{A}\subset\mathscr{B}, \\ \bullet\ \text{We denote by } \alpha_{j_i m} \text{ the coefficient of } X^{h-m}Y^m \\ \text{in } \sigma(F_i)(X,Y)\text{: } \sigma(F_i)(X,Y)=\displaystyle\sum_{m=0}^{h}\alpha_{j_i m}X^{h-m}Y^m. \\ \text{Then, } \det((\alpha_{ij})_{i,j\in J})\neq 0 \text{ (This condition is ignored if } J=\phi), \end{cases}$$

where

$$\sigma(u,v):=(\sigma_{11}u+\sigma_{12}v,\sigma_{21}u+\sigma_{22}v),$$
$$\sigma(F)(X,Y):=F((\sigma^{-1})_{11}X+(\sigma^{-1})_{12}Y,(\sigma^{-1})_{21}X+(\sigma^{-1})_{22}Y),$$

for $(u,v)\in\boldsymbol{R}^2$, $F(X,Y)\in\boldsymbol{R}[X,Y]$, and

$$\sigma=\begin{bmatrix}\sigma_{11} & \sigma_{12}\\ \sigma_{21} & \sigma_{22}\end{bmatrix}\in GL(2,\boldsymbol{R}).$$

Corollary 1 (Tanabe [22]). *Let $\mathscr{C}$ be a Z_4-code with $n_1(\boldsymbol{u})\equiv 0 \pmod 2$ for any $\boldsymbol{u}\in\mathscr{C}$. We use the same notations as in Theorem* 14. *Define*

$$g_1=n-1-\max\{n_2(\upsilon)\mid \upsilon\in C^{\perp} \text{ and } n_1(\upsilon)>0\},$$
$$g_2=\min\{wt_{Hamming}(\upsilon)\mid \upsilon\in C^{\perp} \text{ and } \upsilon\not\equiv 0 \pmod 2\}-1,$$
$$g=\min\{g_1,g_2\}.$$

Let t be an integer with $t\leqslant g$. Assume t satisfies the condition in Theorem 12 *for two linear binary codes $C^{(2)}$ (or its dual) and $(C^{\perp})^{(2)}$ (or its dual). Assume one of the following conditions holds for each k $(1\leqslant k\leqslant t)$:*

(1) *$\Lambda(k)$ satisfies the condition $(*)$ for $(g-k+1,\phi)$.*
(2) *$g_1=g_2=g$, $(g-k+1,n-1-g)\in\Lambda_1(k)$, and $\Lambda(k)$ satisfies the condition $(*)$ for $(g-k+1,\{(X+2Y)^{g-k+1}\})$.*
(3) *$g_1<g_2$ and $\Lambda(k)$ satisfies the condition $(*)$ for $(g-k+1,\{(X+Y)^{g-k+1}\})$.*
(4) *$g_1>g_2$ and $\Lambda(k)$ satisfies the condition $(*)$ for $(g-k+1,\{(X+2Y)^{g-k+1-c}X^c\}_{c=0}^{g-k})$.*

Then, the support of the codewords of $\mathscr{C}$ of any Lee composition $(n_0,n_1,n_2)\in\Gamma(\mathscr{C})$ with $t\leqslant n_1+n_2\leqslant n-t$ forms a t-design and the support of codewords of $\mathscr{C}^{\perp}$ of any Hamming weight l with $l-\lceil l/4\rceil<e$ forms a t-design.

The conditions in the corollary are simple and Tanabe [22] verifies that G_{24} and the lifted quadratic residue code QR_{32} of length 32 satisfy the conditions in the corollary without difficulty. But the corollary cannot find 3-designs in the lifted quadratic residue code of length 48 which were found in [4] and 3-designs in Delsarte–Goethals and Goethals codes over Z_4 which were found in [20,19].

6. Uncited references

[11,24]

References

[1] E.F. Assmus, H.F. Mattson Jr., New 5-designs, J. Combin. Theory 6 (1969) 122–151.
[2] C. Bachoc, On harmonic weight enumerators of binary codes (1999) preprint.
[3] A. Bonnecaze, A.R. Calderbank, P. Solé, Quaternary quadratic residue codes and unimodular lattices, IEEE Trans. Inform. Theory 41 (1995) 366–377.
[4] A. Bonnecaze, E. Rains, P. Solé, 3-Colored 5-designs and Z_4-codes, Research Report No. 4, Royal Melbourne Institute of Technology, Australia, 1998.
[5] A. Bonnecaze, P. Solé, C. Bachoc, B. Mourrain, Type II codes over Z_4, IEEE Trans. Inform. Theory 43 (1997) 969–976.
[6] I. Duursma, T. Helleseth, C. Rong, K. Yang, Split weight enumerators for the Preparata Codes with applications to designs, Designs Codes Cryptogr. 18 (1999) 103–124.
[7] T.A. Gulliver, M. Harada, Extremal double circulant Type II codes over Z_4 and construction of 5-(24, 10, 36) designs, Discrete Math. 194 (1999) 129–137.
[8] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[9] M. Harada, New 5-designs constructed from the lifted Golay code over Z_4, J. Combin. Designs 6 (1998) 225–229.
[10] T. Helleseth, P.V. Kumar, The algebraic decoding of the Z_4-linear Goethals code, IEEE Trans. Inform. Theory 41 (1995) 2040–2048.
[11] T. Helleseth, P.V. Kumar, Sequences with low correlation, in: V. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier Science Publishers, Amsterdam, 1998.
[12] T. Helleseth, P.V. Kumar, K. Yang, An infinite family of 3-designs from Preparata codes over Z_4, Designs Codes Cryptogr. 15 (1998) 175–181.
[13] T. Helleseth, C. Rong, K. Yang, A 3-$(2^5, 7, 105)$ Design from Goethals Codes over Z_4, Reports in Informatics, No. 142, University of Bergen, 1997.
[14] T. Helleseth, C. Rong, K. Yang, New infinite families of 3-designs from Preparata codes over Z_4, Discrete Math. 195 (1-3) (1999) 139–156.
[15] T. Helleseth, C. Rong, K. Yang, New 3-designs from Goethals codes over Z_4, Discrete Math. 226 (2001) 403–409.
[16] D. Kreher, t-designs, $t \geqslant 3$, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[17] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[18] E.M. Rains, N.J.A. Slone, Self-dual codes, in: V. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier Science Publishers, Amsterdam, 1998.
[19] D.J. Shin, P.V. Kumar, T. Helleseth, An Assmus–Mattson-Type approach for identifying 3-designs from linear codes over Z_4 (1998) preprint.
[20] D.J. Shin, P.V. Kumar, T. Helleseth, 3-Designs from the Z_4-Goethals codes via a new Kloosterman sum identity (1998) preprint.
[21] K. Tanabe, An Assmus–Mattson theorem for Z_4-codes, IEEE Trans. Inform. Theory 46 (2000) 48–53.
[22] K. Tanabe, A criterion for designs in Z_4-codes on the symmetrized weight enumerator (1999) preprint.
[23] K. Yang, T. Helleseth, Two new infinite families of 3-designs from Kerdock codes over Z_4, Designs Codes Cryptogr. 15 (1998) 201–214.
[24] K. Yang, T. Helleseth, P.V. Kumar, A. Shanbhag, On the weight hierarchy of Kerdock codes over Z_4, IEEE Trans. Inform. Theory 42 (1996) 1587–1593.
[25] G.V. Zaitsev, V.A. Zinoviev, N.V. Semakov, Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes, in: B.N. Petroc, F. Csáki (Eds.), Second International Symposium on Information Theory, Akadémiai Kiadó, Budapest, 1973, pp. 257–263.